# Symantec™ Encryption Desktop Version 10.3 for Mac OS X Release Notes

Thank you for using this Symantec Corporation product. These Release Notes contain important information regarding this release of Symantec Encryption Desktop for Mac OS X. Symantec Corporation strongly recommends you read this entire document.

Symantec Corporation welcomes your comments and suggestions. You can use the information in Getting Assistance to contact us.

Product: Symantec Encryption Desktop for Mac OS X

Version: 10.3.2

Warning: Export of this software may be restricted by the U.S. government.

Note: To view the most recent version of this document, go to the Products section on the Symantec Corporation Support website.

## What's Included in This File



## About Symantec Encryption Desktop

Symantec™ Encryption Desktop, Powered by PGP Technology is a security tool that uses cryptography to protect your data against unauthorized access.

Symantec Encryption Desktop protects your data while being sent by email. It lets you encrypt your entire hard drive—so everything is protected all the time—or just a portion of your hard drive, via a virtual disk on which you can securely store your most sensitive data. You can use it to share your files and folders securely with others over a network. It lets you put any combination of files and folders into an encrypted, compressed package for easy distribution or backup. Finally, use Symantec Encryption Desktop to shred (securely delete) sensitive files—so that no one can retrieve them—and shred free space on your hard drive, so there are no unsecured remains of any files.

Use Symantec Encryption Desktop to create PGP keypairs and manage both your personal keypairs and the public keys of others.

## Changes in This Release

This section lists the changes in this release of Symantec Encryption Desktop.

### What's New in Symantec Encryption Desktop Version 10.3 for Mac OS X

Building on Symantec Corporation's proven technology, Symantec Encryption Desktop 10.3 for Mac OS X includes numerous improvements and the following new features.

#### What's New in Symantec Encryption Desktop version 10.3.2

- Compatibility with Apple Mac OS X 10.8.5, 10.9, 10.9.1, 10.9.2 and 10.9.3

  This release supports the installation of Symantec Encryption Desktop on systems running Apple Mac OS X 10.8.5, 10.9, 10.9.1, 10.9.2 and 10.9.3. (Note that installation on systems running Mac OS X 10.8.2 and 10.8.3 has been removed.)

As previously announced, we have removed the Instant Messaging feature in Symantec Encryption Desktop.

### What's New in Symantec Encryption Desktop version 10.3.1

- **Compatibility with Apple Mac OS X 10.8.2, 10.8.3, and 10.8.4**

  This release supports installation of Symantec Encryption Desktop on systems running Mac OS X 10.8.2, 10.8.3, and 10.8.4.

Note: Symantec Corporation plans to end-of-life the Instant Messaging Client feature in the next major release of Symantec Encryption Desktop.

### What's New in Symantec Encryption Desktop version 10.3.0

- **Symantec identity branding**

  The PGP product line has been renamed. For a detailed map of old product names to new ones, refer to the Symantec Knowledgebase article TECH197084.

- **Compatibility with Apple Mac OS X 10.8**

  This release supports installation of Symantec Encryption Desktop, formerly known as PGP Desktop, on systems running Mac OS X 10.8 (Mountain Lion).

### Resolved Issues

For a list of issues that have been resolved in this release, please go to the Symantec Knowledgebase and search for TECH166098, "Symantec Encryption Desktop Resolved Issues."

## System Requirements

- Apple Mac OS X 10.8.4, 10.8.5, 10.9, 10.9.1, 10.9.2, 10.9.3
- 512 MB of RAM
- 80 MB hard disk space

Symantec Drive Encryption is not compatible with any third-party software that could bypass the Symantec Drive Encryption protection on the Master Boot Record (MBR) and write to or modify the MBR.

Note: Starting with the release of Symantec Encryption Desktop 10.3.2, Symantec Encryption Desktop will not be compatible with Apple Boot Camp on any Apple Mac OS X system. For more information on upgrading Symantec Encryption Desktop 10.3.2 on Macintosh systems enabled with Apple Boot Camp, go to the Symantec Knowledgebase and search for TECH212700, "Upgrading Symantec Encryption Desktop to version 10.3.2 on Macintosh systems enabled with Apple Boot Camp".

### Compatible Email Client Software

Symantec Encryption Desktop will, in most cases, work without problems with any Internet-standards-based email client that runs on Mac OS X 10.8.4, 10.8.5, 10.9, 10.9.1, 10.9.2 or 10.9.3.

- Apple Mail 5.x, 6.x, 7.x
- Microsoft Outlook for Mac 2011

### Anti-Virus Client Software Compatibility for Macintosh

- **Norton Antivirus 11 and Norton Internet Security 3.0**: To use Symantec Encryption Desktop with email, you must disable the Vulnerability Protection option in Norton. To do this, select Auto Protection and then disable the option for Vulnerability Protection." [18130/2463322]
- **ClamXav**: ClamXav is not compatible with Symantec Drive Encryption on Mac OS X systems. [25682/2470635]
- **VirusBarrier X6**: VirusBarrier X6 is not compatible with Symantec Drive Encryption on Mac OS X systems. [28849/2473805]

# Installation Instructions

To install this release at the same time as you are upgrading the operating system, see the note following the instructions.

The Java Runtime Engine (JRE) is required when installing Symantec Encryption Desktop on Mac OS X. During Symantec Encryption Desktop installation, you are prompted to install the JRE if it is not present on your system. If you choose not to install the JRE, the installation of Symantec Encryption Desktop will not continue.

To install Symantec Encryption Desktop on your Mac OS X system:

1. Mount the Symantec Encryption Desktop disk image.
2. Double-click `Encryption Desktop.pkg`.
3. Follow the on-screen instructions.
4. If prompted to do so, restart your system.

For additional information, including upgrade instructions, see the *Symantec Encryption Desktop for Mac OS X User's Guide*.

Note: If you are upgrading your computer to a new major release of Mac OS X and want to use this version of Symantec Encryption Desktop, be sure to uninstall any previous versions of Symantec encryption software *before* upgrading to the new version of Mac OS X and installing this release. Be sure to back up your keys and keyrings before uninstalling. Note that if you have encrypted your disk, you need to decrypt your disk before you can uninstall Symantec Encryption Desktop or PGP Desktop.

# Licensing

Symantec Encryption Desktop uses a license key to determine what features will be active. You enter your Symantec Encryption Desktop license key using the Setup Assistant after installation. If you are in a domain protected by a Symantec Encryption Management Server, your Symantec Encryption Management Server administrator may have configured your Symantec Encryption Desktop installer with a license key.

For more information about Symantec Encryption Desktop licensing and purchase options, go to the Symantec website.

# Additional Information

## General

- Enrolling to a Symantec Encryption Management Server: When enrolling to a Symantec Encryption Management Server, be sure you are connected to your internal network using a wired connection. Using a VPN connection (such as that with a wireless connection) results in write errors and an incomplete enrollment. [2899819]
- Installation: This version of Symantec Encryption Desktop replaces all older PGP products, as well as replacing PGP Universal Satellite 2.X. These products will be removed as part of upgrading to Symantec Encryption Desktop. [NBN]
- Upgrading the Mac OS X software: If you are upgrading your computer to a new major release of Mac OS X, be sure to uninstall any previous versions of this software *before* upgrading to the new version of Mac OS X. Be sure to back up your keys and keyrings before uninstalling. Note that if the disk is encrypted, you will need to decrypt your disk before you can uninstall. Once you have upgraded your version of Mac OS X, you can then reinstall Symantec Encryption Desktop.
- Upgrading to Symantec Encryption Desktop version 10.3: When upgrading from a previous version (such as from 10.3.1), after rebooting the Mac OS X system, the system may appear to stop with a message "updating boot cache." If this issue occurs, restart the system with hard reboot. The system will boot correctly then. [23955/2468906]
- Enabling shortcut functions from the Finder. In Mac OS X 10.6, Apple changed the way shortcuts are available from the Finder. In order to enable shortcuts to encrypt or sign files, or mount disks, you must first enable the keyboard shortcuts in the Services preferences. To do this, open System Preferences and open the Keyboard option. Select the Keyboard Shortcuts panel and verify the shortcuts are there. Then, to perform any encrypt or sign functions, select the file, choose Finder > Services, and select the appropriate option. [18872/2464065]
- Using RAID volumes: There is a known issue with RAID drives and Mac OS X systems (Apple confirms this issue). When Symantec Encryption Desktop is installed on a system with a RAID volume, you will not be able to properly shut down

the system. Note that if you unmount the volume prior to shutting down the system, the shutdown will complete properly. [25694/2470647]

- Zero byte certificate files. Under certain circumstances, zero byte `cert*.pem` files are created on the root of the disk. You can delete these temporary files as they are not used after installation has completed. [29407/2474363]

## PGP Keys

- Interoperability with older versions of PGP Desktop: PGP Desktop 9.0.X did not have support for DSA key sizes greater than 1024 bits. Users of PGP Desktop 9.0.X cannot properly view the properties of such keys, or create signatures with them, or verify signatures made by them. If interoperability with this version is important, use RSA keys, or DSA keys of 1024 bits. [27905/2472860]
- Adding an ADK to a keypair: When adding an Additional Decryption Key (ADK) to a keypair, do not then create another ADK and add the second ADK to the first keypair. [28420/2473376]
- Using local keyrings: While you can create additional keyrings in Symantec Encryption Desktop, Symantec recommends that you use only the default keyring created during installation of the product. Only the default keyring is used by Symantec Encryption Desktop and keys stored in other keyrings are not used. [2577064]

## PGP Messaging

- Adding new Exchange email accounts: When you add a Microsoft Exchange account in Mail.app, Mail.app automatically selects its server type and uses Exchange Web Service with Port 80 for that email account. As a result, Symantec Encryption Desktop cannot proxy email through the account. To work around this issue, when you add a new Microsoft Exchange account in Mail.app, hold down the Option key after you click Continue when setting up the email account. You can then select IMAP as the Account type. You will not encounter this issue if you are using Thunderbird for your email client on Mac OS X.
- Thunderbird Email Sent to BlackBerry Users: If your Thunderbird email client is set to send email in HTML-only format, and the message is encrypted by either Symantec Encryption Management Server or Symantec Encryption Desktop before it arrives at the BES gateway, the recipient will be unable to view the email message on his or her BlackBerry. To work around this issue, configure your Thunderbird email client so that it does not send HTML-only messages. [16273/2461463]
- Adding comments to secured messages: To ensure proper display of comments added to secured messages using the Add a comment to secured messages option, Symantec Corporation recommends using ASCII text in the Comment field. [11127/2456310]
- S/MIME-signed email messages: Symantec Encryption Desktop may not process S/MIME signed emails if the signing X.509 certificate is not included in the email. The certificate is almost always included with the email unless the sender turns off this option. [9489/2454670, 9491/2454672]
- Automatic mode: Symantec Encryption Desktop is initially installed in Automatic mode. If necessary, you can change this in the Preferences to accommodate your environment. Automatic mode uses Mac OS X's built-in firewall functionality to redirect your email client connections through Symantec Encryption Desktop. Some less common configurations may need to use Manual mode instead. If you fall into the categories below, you should switch to Manual mode in the PGP Preferences (Messaging > Proxy Options > Email). [NBN]

  These include:

  - Those with a requirement to use the built-in firewall for other purposes. Note that third-party applications can be installed to provide much more complete configuration options than the built-in user interface in System Preferences. These other solutions are compatible with Symantec Encryption Desktop. Note that Norton Internet Security 3.0 does not use these methods, and is not compatible with Automatic mode.
  - Those who already redirect their email connections through, for instance, an SSH tunnel or VPN connection. Some VPN connections may cause problems with the connection diversion capabilities of Symantec Encryption Desktop.
  - Automatic mode should *not* be used on a system which is also a mail server; use Manual mode instead.
- Multiple users and Automatic mode: If you fast user switch between multiple Symantec Encryption Desktop users on a single Mac OS X machine, the first user to enable Automatic mode in Symantec Encryption Desktop will be the only user who will be able to use Automatic mode; all other users must use Manual mode. If there are three or more users, each Manual mode user must bind to unique ports. [3335/2448506]
- Mail.App displays a message "Cannot send message using the server [server name]." This message is displayed because Mail.App defaults to forcing using SSL for email. To work around this issue:

  1. When you receive the message in Mail.App, click Edit SMTP Server List.
  2. In the Accounts window, click the Advanced tab, ensure that the option to Use Secure Sockets Layer (SSL) is not

selected, and click OK.

3. Close the Accounts window.

4. In Mail.App, click Try with Selected Server.

Email is sent secured without error messages. [2921285]

## PGP Shredder

- Shredding symbolic links: Shredding symbolic links on the Mac will shred the linked file or directory. [8922/2454102]

## PGP Viewer

- Copying your decrypted message to Inbox. On Mac OS X 10.8.4, you can drag and drop an encrypted email message from Mail.app to PGP Viewer to decrypt and view the message. However, you cannot copy the decrypted message to an Inbox folder using the Copy to Inbox feature of PGP Viewer in this release. [3275948]
- ASCII-armored text. PGP Viewer does not support pasting in ASCII-armored text. To decrypt an email containing ASCII-armored text, drag and drop the entire email message into PGP Viewer. [23202/2468149]
- Displaying Decrypted Messages: If you drag an item to PGP Viewer and the message does not appear, restart PGP Viewer and drag the item again. [22215/2467160]
- Cancelling the passphrase prompt: If you drag an item to PGP Viewer and then click Cancel when prompted to enter your passphrase, you will need to restart PGP Viewer again. This is required so that you can then enter your passphrase in order to decrypt messages. [25390/2470342]
- Viewing attachments with PGP Viewer: Dragging and dropping signed-only messages with attachments directly from Mail.app's IMAP folder is not supported in this release. To view messages with attachments, drag and drop the message to your desktop first before dragging and dropping into PGP Viewer. You can also save the message as an .eml file and drag and drop that file into PGP Viewer. [22806/2467752]

## PGP Virtual Disk

- CAST5 cipher no longer available. The option to use the CAST5 cipher for PGP Virtual Disks has been removed from this release of Symantec Encryption Desktop for Mac OS X. If you have encrypted any virtual disks using this cipher, you will be unable to access that data using this version of Symantec Encryption Desktop. For information on how to access your data using Symantec Encryption Desktop for Windows, or an older version of Symantec Encryption Desktop for Mac OS X, go to the Symantec Knowledgebase and search for TECH204407, "PGP Virtual Disks: Removed Support for CAST5 Cipher." [3123084]
- Unmounting disks on Sleep. The option to prevent sleep if PGP Virtual Disks cannot be unmounted is not working in this release. The system will sleep even if disks cannot be unmounted. [24818/2469770]
- Compacting PGP Virtual Disks: Dynamically sized PGP Virtual Disks created using Symantec Encryption Desktop for Windows cannot be compacted using Symantec Encryption Desktop for Mac OS X on Mac OS X 10.6 systems. [25293/2470245]
- Using case-sensitive journaled, file systems. PGP Virtual Disks formatted as MacOS Extended (Case-sensitive, journaled) may cause problems during shut down when mounted. It is recommended that you close all files and unmount the virtual disk prior to shutting down or restarting the computer. [26477/2471431]

## Symantec Drive Encryption

- Pausing encryption and decryption processes: Do not reboot, or shut down your Mac OS X system while Symantec Encryption Desktop is encrypting or decrypting your disk. If you do so and are unable to reboot your system, you will need to start the system using target disk mode. [25451/2470403]
- Erasing/reformatting encrypted disks: Do not erase or reformat a Symantec Drive Encryption-encrypted disk without decrypting the disk first. [24999/2469951]
- Backwards compatibility. Disks encrypted with this version of Symantec Drive Encryption can only be accessed with version 10.0 for Mac OS X or versions 9.9 and up for Windows. [19875/2464814]
- Backwards compatibility. Disks that use the MBR partition scheme and are encrypted with this version of Symantec Drive Encryption cannot be accessed using older versions of PGP Whole Disk Encryption (version 9.x and earlier). [19875/2464814]
- Fast User Switching. This release of Symantec Encryption Desktop is not compatible with fast user switching on Mac OS X. [23655/2468604]
- External Devices. When plugging in a Samsung Omnia I900 phone to be used as an external storage device, you will

receive a kernel panic and the device will not be mounted. [24353/2469305]

- Universal File System. Disks formatted as UFS are not supported. [23595/2468543]
- Entering Japanese characters. Although the Symantec Encryption Desktop interface allows it, do *not* use Japanese characters when creating Symantec Drive Encryption passphrases as they will not work for authentication at PGP BootGuard. [18139/2463331]
- Encrypting boot disks with both Mac OS X 10.5 and 10.6 installed. Systems booted into Mac OS X 10.5 cannot encrypt a Mac OS X 10.6 disk. To work around this issue, you can boot from Mac OS X 10.6 first and then encrypt the Mac OS X 10.5 disk. [20807/2465747]
- Safe Boot: The Mac OS X Safe Boot feature does not work on a boot disk that has been whole disk encrypted; if you hold down the Shift key to enter Safe Boot, after authenticating at the PGP BootGuard screen, the system will fail to boot. [17770/2462961]
- Symantec Drive Encryption and Recovery Applications: Be sure you decrypt your disk before you run any disk recovery applications (such as DiskWarrior from Alsoft). [18157/2463349]
- Previously Encrypted Partitions or Disks: If you used the PGP Whole Disk Encryption feature of older versions of PGP Desktop for Mac OS X (version 9.x and earlier), you must decrypt those non-boot partitions or disks (including USB flash drives) *before* installing version 10.3 or you will no longer be able to access the data on them. You can re-encrypt the partitions/disks with Symantec Encryption Desktop 10.3 for Mac OS X once it is installed. [NBN]
- Modifying the system partition: Do not make any changes to the system partition on a boot disk that has been encrypted by Symantec Drive Encryption; it will fail to boot properly on the next startup. If you must make changes to the partitioning of an encrypted disk, *decrypt the disk first* and then make the partition changes.
- Supported passphrase characters: [12947/2458134, 18871/2464064] The following characters are supported:

  ```
  abcdefghijklmnopqrstuvwxyz

  ABCDEFGHIJKLMNOPQRSTUVWXYZ

  0123456789

  `~!@#$%^&*()_+={}\|:;[]'"<>,.?/-
  ```

  Most extended characters (such as characters with umlauts) and symbols (such as the registered trademark) are supported.

  Note that in this release, the cent character cannot be entered at boot time at PGP BootGuard.

- Using International Keyboards. Not all keyboards are named the same in different languages. If selecting "English (US-International)" does not work at PGP BootGuard, select "USA." [26286/2471240]
- Using a Mac Mini with Apple Keyboards. The Mac Mini does not have boot time support for the new thin aluminum Apple keyboards. The Symantec Drive Encryption passphrase cannot be entered at boot time using these keyboards with the Mac Mini.
- Partition Formats: APM-formatted disks are not available for encryption. GPT and MBR disks are supported. [11025/2456207]
- Symantec Drive Encryption and NitroAV PCMCIA/Firewire 800 Adaptors: Removable devices connected to a MacBook Pro using a NitroAV PCMCIA/Firewire 800 adapter are not currently supported. [11936/2457121]
- Encrypting Non-Journaled File Systems: Symantec Drive Encryption for Mac OS X does not support "non-journaled" file systems. You will receive an error when trying to encrypt a non-journaled file system. Important note: Previous versions of PGP Whole Disk Encryption for Mac OS X incorrectly allowed the encryption of non-journaled file systems. These disks should be decrypted, backed up, and converted to the Mac OS X default of journaled (non-case sensitive). [19866/2464805]
- Adding keys to removable drives. To add a public key to a removable drive, be sure to add that key to your keyring first. You cannot add public keys to a removable drive if that key is not on your keyring. [20396/2465336]
- Operating system updates during encryption: While your disk is encrypting, do not accept any operating system updates if they are offered. If the update occurs automatically, do not restart your computer until the encryption process has completed. [25451/2470403, 25612/2470565]
- Encrypting Mac OS X formatted external drives with Symantec Drive Encryption for Windows. A drive that is created under Mac OS X using GPT (GUID Partition Table) can be mounted and used on Microsoft Windows systems, but the drive cannot be encrypted using Symantec Drive Encryption for Windows. To work around this issue, either format the disk using MBR Partition or encrypt the disk under Mac OS X. [26460/2471414]
- Software incompatibility with the Symantec Drive Encryption feature: Certain programs are incompatible with the Symantec Drive Encryption feature; do not install these products on a system with Symantec Encryption Desktop, and

do not install Symantec Encryption Desktop on a system with this product installed:

- Faronics Deep Freeze (any edition) [28392/2473348]

- PGP WDE Command Line:
  - Passphrase required for PGP WDE command line stop command: The --stop command now requires a passphrase. Scripts that use this command without providing a passphrase will fail. [29822/2474778]
  - Domain required for PGP WDE command line recovery-configure command: The --recovery-configure command now requires a domain for users that have one. For such users, scripts that use this command without providing a domain will fail. [28656/2473612]
- Compatibility with Apple FileVault: Symantec Drive Encryption functionality is not enabled on systems encrypted using Mac OS X Filevault. To enable Symantec Drive Encryption functionality on these systems, FileVault encryption must be removed and Symantec Drive Encryption must be installed using the Symantec Encryption Desktop installation package. [2824065]
- Encrypting Transcend USB drives: To encrypt an external drive that is not recognized by Symantec Encryption Desktop, such as the Transcend 16GB USB drive, use the Mac OS X Disk Utility to partition and format the drive. [2729560]
- Decrypting on battery power: Do not decrypt an encrypted disk while you are running on battery power. [2734812]

# Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

## Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files

- Troubleshooting that was performed before contacting Symantec
- Recent software configuration changes and network changes

### Licensing and registration

If your Symantec product requires registration or a license key, access our technical support web page at the following URL:

www.symantec.com/business/support/

### Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

### Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

| | |
|---|---|
| Asia-Pacific and Japan | customercare_apac@symantec.com |
| Europe, Middle-East, Africa | semea@symantec.com |
| North America, Latin America | supportsolutions@symantec.com |

## Copyright and Trademarks